

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-037592

(43)Date of publication of application : 07.02.2003

(51)Int.Cl.

H04L 9/32  
H04Q 7/38

(21)Application number : 2001-226237

(71)Applicant : SHARP CORP

(22)Date of filing : 26.07.2001

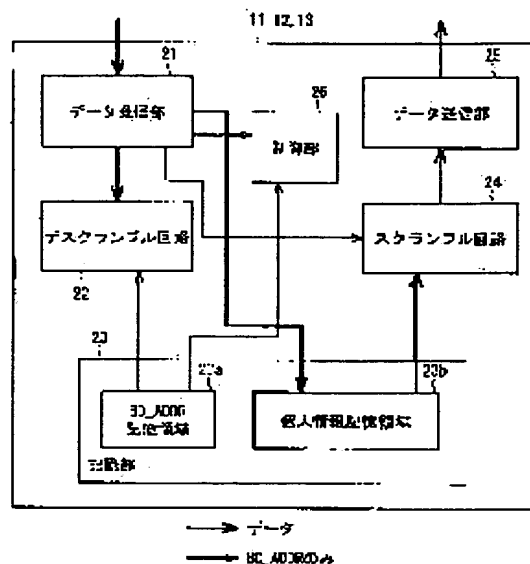
(72)Inventor : MIYASADA HIROSHI

## (54) RADIO COMMUNICATION SYSTEM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To prevent leak or copying of personal information to or by a third party by controlling transfers to other electronic devices when personal information is exchanged between electronic devices capable of radio communication.

**SOLUTION:** A controller 26 of a slave 12 receives a packet 30, confirms its destination BD-ADDR, and judges whether or not it conforms to the slave 12's own BD-ADDR stored in a BD-ADDR storage area 23a. If they conform to each other, the slave 12's BD-ADDR is set to a descramble circuit 22, and the personal information in a field 33 is descrambled and decoded. The personal information is stored in a personal information storage area 23b from a data receiver 21. The master 11 scrambles the information using BD-ADDR of a slave 13 and transfers it to the slave 13.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2003-37592  
(P2003-37592A)

(43) 公開日 平成15年2月7日 (2003.2.7)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 B 5 J 1 0 4
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R 5 K 0 6 7

審査請求 未請求 請求項の数 3 O L (全 5 頁)

(21) 出願番号 特願2001-226237(P2001-226237)

(22) 出願日 平成13年7月26日 (2001.7.26)

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 宮定 浩

大阪府大阪市阿倍野区長池町22番22号 シ

ャープ株式会社内

(74) 代理人 100112335

弁理士 藤本 英介

Fターム(参考) 5J104 AA07 BA04 KA02 KA07 NA01

5K067 AA30 BB21 CC08 CC10 DD17

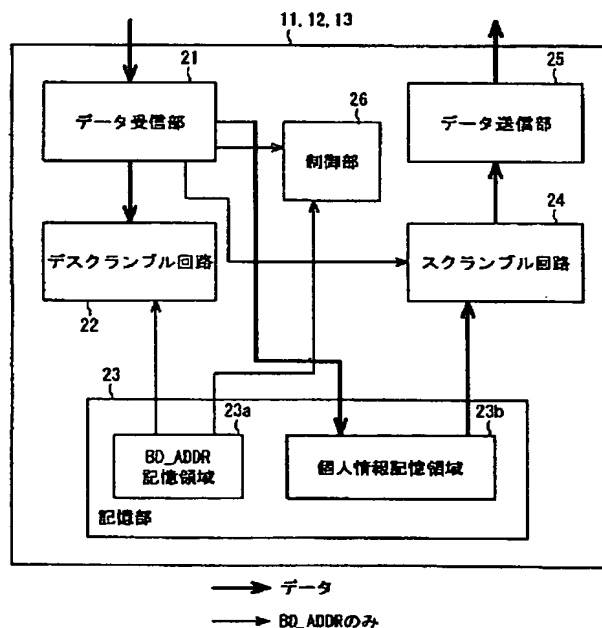
EE02 EE25 HH22 HH23

(54) 【発明の名称】 無線通信装置

(57) 【要約】

【課題】 無線通信が可能な電子機器どうしで個人情報を交換する際に、他の電子機器への転送を抑制することにより、第三者への個人情報の流出や複製を防止する。

【解決手段】 このパケット30を受信したスレーブ12の制御部26は、送信先BD\_ADDRを確認し、BD\_ADDR記憶領域23aに格納されているスレーブ12の固有のBD\_ADDRと一致するか否かを判断する。一致した場合は、スレーブ12のBD\_ADDRをデスクランブル回路22にセットし、フィールド33の個人情報をデスクランブル回路22によりデスクランブルを行って解読する。個人情報は、データ受信部21から個人情報記憶領域23bに格納される。マスター11は、個人情報にスレーブ13のBD\_ADDRを用いてスクランブルをかけてスレーブ13へ転送する。



## 【特許請求の範囲】

【請求項1】 装置固有のパラメータによりデータをスクランブル/デスクランブル可能な無線通信装置において、

送信先装置の第1のパラメータと、前記第1のパラメータによりスクランブルされた情報とを含むデータ信号を受信する受信手段と、

装置自身の固有の第2のパラメータを予め記憶しているパラメータ記憶手段と、

前記第1のパラメータと第2のパラメータが一致しているかを判定する判定手段と、

前記判定手段が一致していると判定した場合に、前記パラメータ記憶手段に記憶されている第2のパラメータにより前記情報にデスクランブルをかけて解読するデスクランブル手段と、

前記判定手段が一致していると判定した場合に、受信した前記情報を記憶する情報記憶手段と、

前記情報記憶手段に記憶された情報をさらに他の装置に送信する場合、該他の送信先装置の第3のパラメータにより前記情報記憶手段に記憶された情報をさらにスクランブルするスクランブル手段と、

送信先装置の前記第3のパラメータと、前記スクランブル手段が第3のパラメータによりスクランブルした情報を含むデータ信号を送信する送信手段とを備えることを特徴とする無線通信装置。

【請求項2】 前記受信手段は、前記第1のパラメータを受信し、前記判定手段が一致していると判断した場合にのみ残りのデータ信号をすべて受信することを特徴とする請求項1記載の無線通信装置。

【請求項3】 Bluetoothによる無線通信を利用し、前記パラメータはBD\_ADDRであることを特徴とする請求項1又は2記載の無線通信装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、PDA(Personal Digital assistants)等の電子機器間同士で情報交換が可能な無線通信装置に関し、特にBluetoothによる通信が可能な電子機器どうして個人情報を交換する際に、Bluetooth機器がもつ特徴を利用したある制限をかけることにより、第三者への個人情報の流出や複製を防止することができる無線通信装置である。

## 【0002】

【従来の技術】近年、PDA等の電子機器を用い、インターネット等を介して情報を交換することが可能となっている。そして、得た情報は、簡単に他の電子機器への転送が自由に行うことができる。

## 【0003】

【発明が解決しようとする課題】このように、電子機器を用いて個人情報を交換した場合、相手側の電子機器から他の電子機器への転送が自由に行えるため、個人情報

2

が直接交換した相手以外の第三者へ転送されたり複製されるなどして、利用されるという状況にあった。

【0004】本発明の目的は、Bluetooth等による無線通信が可能な電子機器どうして個人情報を交換する際に、他の電子機器への転送を抑制することにより、第三者への個人情報の流出や複製を防止する無線通信装置を提供することにある。

## 【0005】

【課題を解決するための手段】本発明は、装置固有のパラメータによりデータをスクランブル/デスクランブル可能な無線通信装置において、送信先装置の第1のパラメータと、前記第1のパラメータによりスクランブルされた情報とを含むデータ信号を受信する受信手段と、装置自身の固有の第2のパラメータを予め記憶しているパラメータ記憶手段と、前記第1のパラメータと第2のパラメータが一致しているかを判定する判定手段と、前記判定手段が一致していると判定した場合に、前記パラメータ記憶手段に記憶されている第2のパラメータにより前記情報にデスクランブルをかけて解読するデスクランブル手段と、前記判定手段が一致していると判定した場合に、受信した前記情報を記憶する情報記憶手段と、前記情報記憶手段に記憶された情報をさらに他の装置に送信する場合、該他の送信先装置の第3のパラメータにより前記情報記憶手段に記憶された情報をさらにスクランブルするスクランブル手段と、送信先装置の前記第3のパラメータと、前記スクランブル手段が第3のパラメータによりスクランブルした情報を含むデータ信号を送信する送信手段とを備えることを特徴とする。

【0006】前記受信手段は、前記第1のパラメータを受信し、前記判定手段が一致していると判断した場合にのみ残りのデータ信号をすべて受信することを特徴とする。

【0007】本発明は、Bluetoothによる無線通信を利用し、前記パラメータはBD\_ADDRであることを特徴とする。

【0008】本発明では、Bluetooth等の無線通信装置同士の個人情報交換において、スクランブル/デスクランブルを行うパラメータを利用して、第三者への個人情報の流出や複製の防止を実現する。すなわち、受信した送信先の第1のパラメータと、あらかじめ記憶しておいた装置自身の固有の第2のパラメータが一致した場合は、デスクランブル手段が第2のパラメータにより解読が可能となる。したがって、第1と第2のパラメータが一致しない場合は、解読できない。また、他の送信先へ、受信した情報を転送しようとした場合、記憶手段に記憶され第1のパラメータでスクランブルされた情報を、さらに送信先の装置固有の第3のパラメータでスクランブルする。このため、この情報を受け取った送信先の装置は、装置固有のパラメータでデスクランブルをかけても、第1のパラメータでスクランブルされている

ので、第1のパラメータを備えていない送信先装置は解読できない。

【0009】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。図1は本発明に係るBluetooth無線通信装置を用いたネットワークを示す構成図である。Bluetooth機器11、12、13を用いたネットワークをピコネット10と呼ぶ。Bluetooth機器11はマスター、Bluetooth機器12、13はスレーブである。

【0010】マスター11はピコネット10の形成に主導的役割を果たす。スレーブ12、13は、ピコネットを形成しようとするマスター11に応答することによって、ピコネットを形成するメンバーとなる。このときマスター11とスレーブ12、13は、互いのBD\_ADDR（パラメータ）を把握している。

【0011】図2は、Bluetooth機器を示すブロック図である。Bluetooth機器11、12、13は、データ受信部21、デスクランブル回路22と、記憶部23と、スクランブル回路24と、データ送信部25と、制御部26とを備える。記憶部23は、BD\_ADDR記憶領域23aと個人情報記憶領域23bを備えている。また制御部26は各部の制御を行う役割を担っている。

【0012】次に、図1に示すピコネット10におけるBluetooth機器の動作について説明する。まずマスター11が、スレーブ12へ個人情報を送信する場合を想定する。マスター11は、データ送信部25からデータ信号を送信する。図3は、個人情報を交換する際に送受信されるデータ信号のパケットの基本構成である。31は送信先ユニットのBD\_ADDRを含むヘッダ、32は送信元ユニットのBD\_ADDRを含むフィールド、33は送信元ユニットの個人情報を含むフィールドである。

【0013】すなわち、マスター11は、図3のフィールド31にスレーブ12のBD\_ADDRを含むヘッダを置き、次にフィールド32にマスター11のBD\_ADDRを、フィールド33に個人情報を書き込んでパケット30を構成し、送信する。このときフィールド33の個人情報データは、送信先であるスレーブ12のBD\_ADDRをセットしたスクランブル回路24でスクランブルがかけられて、データ送信部25に送られ、スレーブ12へ送信される。

【0014】このパケット30を受信したスレーブ12の制御部26は、まずフィールド31に含まれている送信先BD\_ADDRを確認し、BD\_ADDR記憶領域23aに格納されているスレーブ12の固有のBD\_ADDRと一致するか否かを判断する。一致しない場合、制御部26は、データ受信部21に、そのパケットに対する受信動作を行わず、待ち受け状態に戻す。一致し

た場合は、スレーブ12のBD\_ADDRをデスクランブル回路22にセットし、フィールド33の個人情報をデスクランブル回路22によりデスクランブルを行って解読する。

【0015】但し、個人情報データの保存は、フィールド33のスクランブルがかかった状態で保存する。すなわち、個人情報は、フィールド31のBD\_ADDRと、BD\_ADDR記憶領域23aのスレーブ12のBD\_ADDRとが一致した場合に、データ受信部21から個人情報記憶領域23bに格納される。個人情報を参照する際には、デスクランブル回路22により随時デスクランブルを行ない解読する。

【0016】スレーブ12からマスター11へ個人情報を送信する場合も同様である。スレーブ12は通信相手であるマスター11のBD\_ADDRをデータ受信部21で取得し、これをスクランブル回路24のパラメータとしてセットする。スレーブ12の個人情報はこのスクランブル回路24を経てマスター11へ送信される。マスター11はスレーブ12から受け取った個人情報に、自身のBD\_ADDRをパラメータとするデスクランブル回路22を用いて、デスクランブルを行うことで解読する。

【0017】以下、スレーブ12からマスター11へ個人情報を送信した場合の操作手順を箇条書きにして説明する。

1. マスター11とスレーブ12が個人情報を交換する場合、マスター11側では所定の操作することにより個人情報交換のためのアプリケーションを起動し、スレーブ12に対して個人情報交換要求を行う。

2. スレーブ12側も同様に所定の操作によってアプリケーションを起動し、マスター11に対して個人情報交換要求の受理を知らせる。

3. マスター11は要求が受け付けられたことを認識すると、データ送信部25では図3のパケット構成を行って個人情報を送信し、同時にデータ受信部21を起動してスレーブ12からの個人情報送信を待つ。

4. スレーブ12はマスター11からパケットを受信するとデータ受信部21で上記のパケット分解を開始すると共に、データ送信部25を起動してパケット構成を行ない個人情報を送信する。

5. マスター11はスレーブ12からパケットを受信すると、パケット分解を行う。

【0018】次に、マスター11が別のBluetooth機器をスレーブ13としてピコネット10に加え、スレーブ12から受け取った個人情報をスレーブ13に転送した場合について説明する。マスター11とスレーブ13は互いのBD\_ADDRを把握しており、上記手順と同様にしてマスター11は、スレーブ12から受け取った個人情報にスレーブ13のBD\_ADDRを用いてスクランブルをかけてスレーブ13へ転送することは

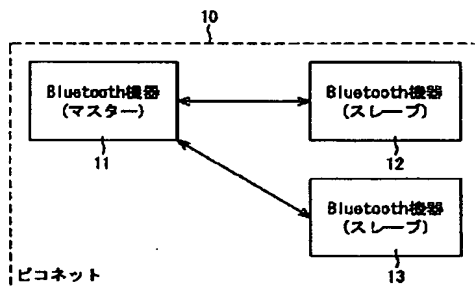
可能である。

【0019】しかしマスター11が保有するスレーブ12の個人情報、マスター11のBD\_ADDRを用いてスクランブルがかけられたものであり、マスター11はこれにスレーブ13のBD\_ADDRを用いてスクランブルをかけて転送するため、スレーブ13は受け取った個人情報に自身のBD\_ADDRを用いてデスクランブルをかけても、マスター11のBD\_ADDRによるスクランブルが解けず、スレーブ12の個人情報が解読できない。このようにして、スレーブ12の個人情報はマスター11以外のBluetooth機器では解読不可能となり、第三者への流出や複製が防止される。

【0020】

【発明の効果】以上のように本発明によれば、受信した送信先の第1のパラメータと、あらかじめ記憶しておいた装置自身の固有の第2のパラメータが一致した場合のみ、デスクランブル手段が第2のパラメータにより解読が可能となる。また、他の送信先へ、受信した情報を転送しようとした場合、記憶手段に記憶され第1のパラメータでスクランブルされた情報を、さらに送信先の装置固有の第3のパラメータでスクランブルするので、この情報を受け取った送信先の装置は、装置固有のパラメータでデスクランブルをかけただけでは、解読できない。このように、無線通信装置どうしでの個人情報交換において、第三者への個人情報の流出や複製の防止を実現す

【図1】



ることができる。

【図面の簡単な説明】

【図1】本発明に係る無線通信装置を用いたネットワークを示す構成図である。

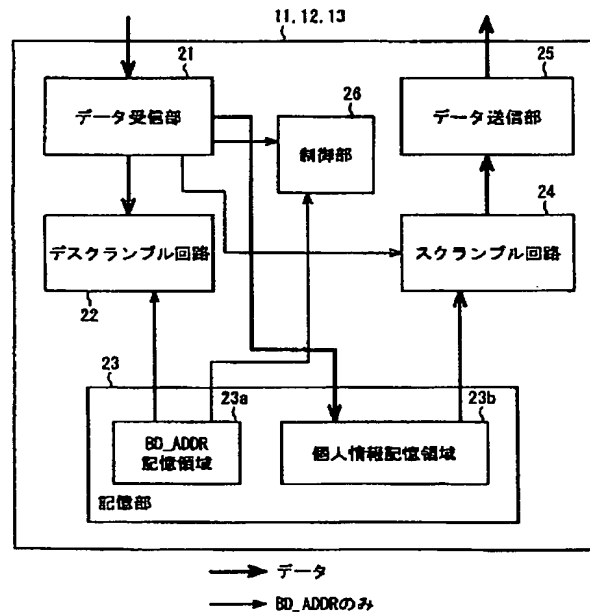
【図2】図1のネットワークを構成するBluetooth機器を示すブロック図である。

【図3】個人情報を交換する際に送受信されるパケットの基本構成図である。

【符号の説明】

- 10 ピコネット
- 11 マスター (Bluetooth機器)
- 12, 13 スレーブ (Bluetooth機器)
- 21 データ受信部
- 22 デスクランブル回路
- 23 記憶部
- 23a BD\_ADDR記憶領域
- 23b 個人情報記憶領域
- 24 スクランブル回路
- 25 データ送信部
- 26 制御部
- 30 パケット
- 31 フィールド
- 32 フィールド
- 33 フィールド/スクランブル

【図2】



【図3】

